THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

LEVI COMBS and ESTEBAN TRUJILLO, on behalf of themselves and all others similarly situated, Plaintiffs, vs. WARNER MUSIC GROUP CORP., Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Levi Combs and Esteban Trujillo ("Plaintiffs") bring this Class Action Complaint against Warner Music Group ("WMG" or "Defendant"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against WMG for its failure to properly secure and safeguard personal identifiable information, including without limitation, unencrypted names, email addresses, telephone numbers, billing addresses, shipping addresses, payment card numbers, payment card CVV security codes, and payment card expiration dates (collectively "PII"). Plaintiffs also allege WMG failed to provide timely, accurate, and adequate notice to Plaintiffs and similarly situated WMG customers ("Class Members") that their PII had been stolen by hackers, and precisely what types of information was unencrypted and in the possession of unknown, unauthorized third parties.

2. WMG owns and operates some of the largest record labels in the world, including Atlantic Records, Elektra Records, Warner Records, and Parlophone. WMG also owns Warner Chappell Music, one of the world's largest music publishers. WMG represents over 60,000 artists.

In marketing its artists' music and other merchandize online, WMG operates thousands of "official" websites for many of its labels and performers. These websites each include an e-commerce platform to assist fans in purchasing music and related merchandise that is operated by WMG and its agents.

3. On or about September 2, 2020, WMG began notifying various state Attorneys General about a data breach that occurred on many of its websites between April 25, 2020 and August 5, 2020 (the "Data Breach"). Around the same time, Defendant mailed a *Notice of Data Breach* to consumers affected by the breach. The notice stated that "an unauthorized third party had compromised a number of US-based e-commerce websites WMG operates," and that this Data Breach allowed the "unauthorized third party" to acquire PII that WMG customers entered into one or more of the affected websites' e-commerce platforms. WMG admitted that the "compromised" PII included full names, email addresses, telephone numbers, billing addresses, shipping addresses, payment card numbers, payment card CVV security codes, and payment card expiration dates.

4. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the Class Members' PII, WMG assumed legal and equitable duties to those consumers. WMG admits that the PII entered onto its websites' e-commerce platforms was "compromised" by "an unauthorized third party." The stolen information includes everything unauthorized third parties need to illegally use WMG's current and former customers' PII to steal their identities and to make fraudulent purchases.

5. Not only can unauthorized third parties access Defendant's customers' PII, the PII can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to other criminals. Plaintiffs and WMG's current and former customers face a lifetime risk of

identity theft and financial crimes.

6. This PII was compromised due to WMG's negligent and/or careless acts and omissions and the failure to protect customers' data. In addition to WMG's failure to prevent the Data Breach, Defendant failed to detect the Data Breach for almost four months, and when WMG did discover the Data Breach, it took at least a month to report it to the affected consumers and the states' Attorneys General.

7. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm. This risk will persist.

8. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of WMG's failure to: (i) adequately protect its customers' PII; (ii) warn customers of its inadequate information security practices; and (iii) effectively monitor its websites and e-commerce platforms for security vulnerabilities and incidents. WMG's conduct amounts to negligence and violates federal and state statutes.

9. Plaintiffs and Class Members have suffered injury as a result of WMG's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, financial crimes, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under the New York Consumer Law for Deceptive Acts and Practices (New York Gen. Bus. Law § 349); and (v) the continued and certainly an increased risk to their PII, which may remain available on the dark web for individuals to access and abuse, and remains in WMG's possession and is subject to further unauthorized disclosures so long as WMG fails to

undertake appropriate and adequate measures to protect these consumers' PII.

10. WMG disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that its customers' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data. As a result, Plaintiffs' and Class Members' PII was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES & CITIZENSHIP

11. Plaintiff Levi Combs is a citizen of Ohio residing in Marysville, Ohio. Mr. Combs purchased items from websites operated by WMG on or about July 20, 2020 and July 23, 2020. He used a payment card for the purchases. He received email confirmations of both purchases directly from WMG. He received WMG's *Notice of Data Breach*, dated September 3, 2020, on or about September 8, 2020.

12. Plaintiff Esteban Trujillo is a citizen of Florida residing in Orlando, Florida. Mr. Trujillo purchased an item from a website operated by WMG on or about May 28, 2020. He used a payment card for the purchase. He received an email confirmation of the purchase directly from WMG. Mr. Trujillo received WMG's *Notice of Data Breach*, dated September 3, 2020, on or about September 9, 2020

13. Defendant Warner Music Group Corp. is a Delaware corporation with its principal place of business in New York, New York. Therefore, WMG is a citizen of both Delaware and

New York.

14. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

15. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

16. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member (Plaintiff Levi Combs is a citizen of Ohio and Plaintiff Esteban Trujillo is a citizen of Florida) is a citizen of a state different from Defendant to establish minimal diversity.

17. The Southern District of New York has personal jurisdiction over WMG because WMG is headquartered in this District and conducts substantial business in New York and this District through its headquarters, offices, and affiliates.

18. Venue is proper in this District under 28 U.S.C. §1391(b) because WMG is headquartered in this District and a substantial amount of the WMG's conduct harming Plaintiffs and Class Members originated from this District.

IV. FACTUAL ALLEGATIONS

Background

19. WMG is an American multinational entertainment and record label conglomerate

based in New York City. As one of the "big three" recording companies in the global music industry, WMG operates thousands of websites with e-commerce platforms. With a multibillion-dollar annual turnover, WMG represents over 60,000 artists, employs more than 3,500 people, and has operations in more than 50 countries. WMG owns and operates some of the largest and most successful labels in the world, including Atlantic Records, Elektra Records, Warner Records, and Parlophone.

20. Formerly part of Time Warner, WMG was publicly traded on the New York Stock Exchange until 2011 when it announced its privatization and sale to Access Industries. Earlier this year, WMG had its second IPO on Nasdaq, once again becoming a public company.

21. Plaintiffs and the Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Customers demand security to safeguard their PII.

22. WMG had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties. WMG touts the secure nature of its websites in its various Privacy Policies, including the one provided by Atlantic Records: "We will use reasonable physical, technical and administrative measures to protect Personal Information under our control." WMG also states: "We want to emphasize at the outset that keeping personal information safe and secure is very important to us."[1]

23. WMG does not claim that it abides by the PCI DSS (Payment Card Industry Data Security Standard) compliance. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions. Businesses that

[1] *Notice of Data Breach*, filed Sept. 2, 2020 with the California Attorney General, a true and correct copy of which is attached hereto as Exhibit 1 ("Ex. 1").

fail to maintain PCI DSS compliance are subject to steep fines and penalties.

24. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: Developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks using anti-virus software and updating it regularly.[2]

25. To purchase items on WMG's websites, customers can either create an account or check out as a guest. Either choice requires, at a minimum, that the customer enter the following PII onto the website:

- Full name;
- billing address;
- shipping address;
- email address;
- telephone number;
- name on the payment card;
- type of payment card;
- full payment card number;
- payment card expiration date; and
- security code, or CVV code (card verification number).

26. When a customer purchases items on WMG's websites, as a guest or through an account, when they enter their PII at the initial sign-up screen they are not asked to acknowledge a "Privacy Policy," and they are not asked to read the "Terms of Use." There is only a statement in uniform font that reads: "By placing this order, you agree to our Terms, Conditions and Cancellation Policy." Links to WMG's "Privacy Policy" and "Terms of Use" are included on the extreme bottom right borders of the website pages in unremarkable font, with no indications of hyperlinks to the policies or terms. The "Privacy Policy" and "Terms of Use," however, do not appear at all on the mobile webpage unless the user clicks on another link. Similarly, there are no

[2] PCI Security Standards Council, available at: https://www.pcisecuritystandards.org/ (last accessed Sept. 9, 2020).

links to the "Terms of Use" on the e-commerce platform where the purchase is finalized.

The Data Breach

27. Beginning on or about September 3, 2020, WMG sent customers a *Notice of Data Breach*.[3] WMG, identifying itself as "Warner Music Group 1633 Broadway New York, NY 10019," informed the recipients of the notice that:

> **WHAT HAPPENED?**
> On August 5, 2020, we learned that an unauthorized third party had compromised a number of US-based e-commerce websites WMG operates but that are hosted and supported by an external service provider. This allowed the unauthorized third party to potentially acquire a copy of the personal information you entered into one or more of the affected website(s) between April 25, 2020 and August 5, 2020.
>
> **WHAT INFORMATION WAS INVOLVED?**
> Any personal information you entered into one or more of the affected website(s) between April 25, 2020 and August 5, 2020 after placing an item in your shopping cart was potentially acquired by the unauthorized third party. This could have included your name, email address, telephone number, billing address, shipping address, and payment card details (card number, CVC/CVV and expiration date).

28. On or about September 2, 2020, WMG sent letters detailing the Data Breach to various state Attorneys General, including Iowa's Attorney General. In that letter, WMG confirmed the information in the *Notice of Data Breach*, but added that the unauthorized third party that "compromised" WMG's e-commerce websites "acquired a copy of information customers entered on the affected websites after [the customers] plac[ed] an item into their shopping carts."[4]

29. WMG admits it did not detect the Data Breach for more than three months. WMG's customers' PII was scraped by hackers and available to other criminals and, on information and

[3] *Notice of Data Breach*, filed Sept. 2, 2020 with the California Attorney General, a true and correct copy of which is attached hereto as Exhibit 1 ("Ex. 1").
[4] *Letter to Iowa's Consumer Protection Division, Office of the Attorney General*, Sept. 2, 2020, *available at*: https://www.iowaattorneygeneral.gov/media/cms/922020_Warner_Music_Group_74089CCFA8DE1.pdf (last accessed Sept. 10, 2020).

belief, may still be for sale to criminals on the dark web. Even though WMG promised consumers it uses "reasonable physical, technical and administrative measures to protect Personal Information under our control," unauthorized individuals accessed WMG's customers' PII.

30. In response to the Data Breach, WMG claims it "took steps to address and correct the issue. We also notified the relevant credit card providers as well as law enforcement[.]" WMG is also offering affected customers one year of "identity monitoring services," but there is no offer of identity theft insurance.

31. WMG did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for current and former customers, causing Plaintiffs' and Class Members' PII to be exposed.

Scraping and E-Skimming Breaches

32. Magecart is a loose affiliation of hacker groups responsible for skimming payment card attacks on various companies, including British Airways and Ticketmaster.[5] Typically, these hackers insert virtual credit card skimmers or scrapers (also known as *formjacking*) into a web application (usually the shopping cart), and proceed to scrape payment card information to sell on the dark web.[6]

33. The hackers target what they refer to as the fullz; a term used by criminals to refer to stealing the full primary account number, card holder contact information, credit card number, CVC/CVV code, and expiration date. The fullz is exactly what WMG admits the malware infecting its e-commerce platform scraped.

34. These cyber-attacks exploit weaknesses in the code of the e-commerce platform,

[5] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost, Aug. 28, 2019, *available at:* https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ (last accessed Sept. 9, 2020).
[6] *Id.*

without necessarily comprising the victim website's network or server.[7]

35. Magecart and these scraping breaches are not new: RiskIQ's earliest Magecart observation occurred on August 8, 2010, and only continued to proliferate over the last decade.[8] Thus, WMG would have been made aware of this type of breach since that time, especially considering the surge of these types of breaches in the last few years.

36. Unfortunately, despite all of the publicly available knowledge of the continued compromises of PII in this manner, WMG's approach to maintaining the privacy and security of Plaintiffs' and Class members' PII was at the very least negligent, as WMG did not maintain reasonable security procedures and practices appropriate to the nature of the information to protect consumers' valuable PII.

Securing PII and Preventing Breaches

37. WMG could have prevented this Data Breach by properly encrypting the PII or appropriately and adequately monitoring the e-commerce platforms for malicious codes. The code in this case was in place for over three months. WMG's negligence in safeguarding its customers' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing e-commerce platforms across the country and to corporations alike. And WMG, specifically, has suffered similar breaches as recently as 2017.[9]

38. WMG has acknowledged the sensitive and confidential nature of the PII. Despite the prevalence of public announcements of data breaches and data security compromises, and despite its own acknowledgments of data security compromises, and despite acknowledgment of

[7] *What is Magecart and was it behind the Ticketmaster and BA hacks?*, Computerworld, Sep. 18, 2018, *available at*: https://www.idgconnect.com/idgconnect/news/1029449/magecart-ticketmaster-hacks (last accessed Sept. 9, 2020).
[8] *Magecart: New Research Shows the State of a Growing Threat*, RiskIQ, Oct. 4, 2019, *available at*: https://www.riskiq.com/blog/external-threat-management/magecart-growing-threat/ (last accessed Sept. 9, 2020).
[9] *Lax Security Exposes 4 Million Warner Bros Customers' Data*, Identiy Theft Resource Center, *available at*: https://www.idtheftcenter.org/lax-security-exposes-4-million-warner-bros-customers-data/ (last accessed Sept. 9, 2020).

its duties to keep PII private and secure, WMG failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

39. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[11]

40. The ramifications of WMG's failure to keep its customers PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

41. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[13]

42. At all relevant times, WMG knew, or reasonably should have known, of the

[10] 17 C.F.R. § 248.201 (2013).
[11] *Id*.
[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Sept. 10, 2020).
[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Sept. 10, 2020).

importance of safeguarding PII and of the foreseeable consequences that would occur if its data security systems were breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

43. WMG was, or should have been, fully aware of the significant volume of daily payment card transactions on its websites. The malware infected WMG's e-commerce platforms where customers could purchase or reserve certain products only available through Defendant's websites, amounting to potentially millions of payment card transactions exposed to malicious actors.

44. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

45. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

46. To date, WMG has offered its customers only one year of credit monitoring service, with no identity theft insurance. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come.

47. The injuries to Plaintiffs and Class Members were directly and proximately caused

[14] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last visited Sept. 9, 2020).

by WMG's failure to implement or maintain reasonable, adequate data security measures for its customers' PII.

Plaintiff Combs' Experience

48. Plaintiff Levi Combs accessed one of Defendant's websites on or about July 20, 2020 and purchased items for approximately $30 on his payment card. On or about July 23, 2020, he accessed that website again and used his payment card to purchase another item for approximately $30.

49. Mr. Combs made these purchases through websites operated by WMG. He entered his PII into WMG's e-commerce payment platform, including his full name, billing and shipping addresses, payment card types and full numbers, CVV codes, payment card expiration dates, email address, and telephone number.

50. Mr. Combs received the *Notice of Data Breach*, dated September 3, 2020, on or about September 8, 2020. He did not receive the notice by email.

51. On or about August 28, 2020, unknown third parties used Mr. Combs' payment card—the same payment card he used on WMG's hacked e-commerce platform—to make an unauthorized purchase via the internet. The purchase totaled $197.90. The money was withdrawn from Mr. Combs' checking account in August 2020, and although his bank confirmed the charges were unauthorized, the losses were not fully reimbursed by the bank until one or two days later, depriving Mr. Combs of the financial benefit of that $197.90 deficit.

52. As a result of the Data Breach and the theft of his funds, Mr. Combs spent time dealing with the consequences of the Data Breach, which includes time spent confirming that he made purchases using his payment card during the relevant period, reviewing his accounts, including the account compromised by the Data Breach, contacting his bank, self-monitoring his

accounts, and exploring credit monitoring and identity theft insurance options.

53. Mr. Combs is not aware of any other data breaches that could have resulted in the theft of his payment card information. He is very careful about sharing his PII, selecting reputable vendors and merchants, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

54. Mr. Combs stores any and all documents containing his PII in a safe and secure digital location, and destroys any documents he receives in the mail that contain his PII, or that may contain any information that could otherwise be used to compromise his payment card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

55. Mr. Combs suffered actual injury and damages in losing at least $197.90 from his bank account, and in paying money to, and purchasing products from, WMG's websites during the Data Breach; expenditures which he would not have made had WMG disclosed that it lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

56. Mr. Combs suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to WMG for the purpose of purchasing WMG's products and which was compromised in and as a result of the Data Breach.

57. Mr. Combs suffered lost money, time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of his privacy.

58. Mr. Combs has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

59. Mr. Combs has a continuing interest in ensuring that his PII, which, upon

information and belief, remains backed up in WMG's possession, is protected and safeguarded from future breaches.

Plaintiff Trujillo's Experience

60. Plaintiff Esteban Trujillo accessed one of WMG's websites and purchased items for approximately $30 on his payment card.

61. Mr. Trujillo made this purchases through a website operated by WMG. He entered his PII into WMG's e-commerce payment platform, including his full name, billing and shipping addresses, payment card type and full number, CVV code, payment card expiration date, email address, and telephone number.

62. Mr. Trujillo received the *Notice of Data Breach*, dated September 3, 2020, on or about September 9, 2020. He did not receive the notice by email.

63. On or about August 6, 2020, unknown third parties used Mr. Trujillo's payment card—the same payment card he used on WMG's hacked e-commerce platform—to make an unauthorized purchase via the internet. The purchase totaled $86.11. Mr. Trujillo's bank notified him that the purchase was suspicious and declined the charge.

64. As a result of the Data Breach and undeniable theft and misuse of his payment card information, Mr. Trujillo spent time dealing with the consequences of the Data Breach, which includes time spent confirming that he made purchases using his payment card during the relevant period, reviewing his accounts, including the account compromised by the Data Breach, contacting his bank, self-monitoring his accounts, and exploring credit monitoring and identity theft insurance options.

65. Mr. Trujillo is not aware of any other data breaches that could have resulted in the theft of his payment card information. He is very careful about sharing his PII, selecting reputable

vendors and merchants, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

66. Mr. Trujillo stores any and all documents containing his PII in a safe and secure digital location, and destroys any documents he receives in the mail that contain his PII, or that may contain any information that could otherwise be used to compromise his payment card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

67. Mr. Trujillo suffered fraud, and in paying money to, and purchasing products from, WMG's websites during the Data Breach; expenditures which he would not have made had WMG disclosed that it lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

68. Mr. Trujillo suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to WMG for the purpose of purchasing WMG's products and which was compromised in and as a result of the Data Breach.

69. Mr. Trujillo suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of his privacy.

70. Mr. Trujillo has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

71. Mr. Trujillo has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in WMG's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

72. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

73. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII was compromised in the data breach first announced by Warner Music Group on or about September 3, 2020 (the "Nationwide Class").

74. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their staff and immediate family members.

75. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

76. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class is so numerous that joinder of all members is impracticable. Upon information and belief, Defendant has records sufficient to determine and identify those consumers who comprise the Class.

77. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to statutory damages, compensatory damages, consequential damages, nominal damages, and/or punitive damages as a result of Defendant's wrongful conduct.

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

78. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach due to Defendant's misfeasance.

79. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

80. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

81. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their

common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

82. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

83. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

84. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

85. Unless a Class-wide injunction is issued, Defendant may continue in its failure to

properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth herein.

86. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

87. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing

to safeguard the PII of Plaintiffs and Class Members; and,

g. Whether Class Members are entitled to statutory damages, compensatory damages, consequential damages, nominal damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

88. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 87.

89. As a condition of their using the services of Defendant, customers were obligated to provide Defendant with their PII, including payment card information.

90. Plaintiffs and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

91. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

92. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its customers' PII involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

93. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and Class Members' PII in Defendant's

possession was adequately secured and protected.

94. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

95. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and previous breach incidents involving its customers' PII.

96. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

97. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' PII.

98. Plaintiffs and the Class Members had no ability to protect their PII that was in, and upon information and belief remains in, Defendant's possession.

99. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

100. Defendant had and continues to have a duty to adequately disclose the details of the Data Breach sufficient to allow Plaintiffs and the Class Members to take steps to prevent, mitigate, and repair any identity theft, financial fraud, and the fraudulent use of their PII by third parties.

101. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

102. Defendant has admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

103. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within Defendant's possession or control.

104. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

105. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect customers' PII in the face of increased risk of theft.

106. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its customers' PII.

107. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

108. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

109. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and Class Members and the harm suffered or risk

of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

110. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, financial fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from financial crimes and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

111. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

112. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 87.

113. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

114. Defendant owed a duty to its customers, including Plaintiffs and Class Members, to keep their PII contained as a part thereof, confidential.

115. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiffs and Class Members.

116. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and Class Members, by way of Defendant's failure to protect the PII.

117. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members is highly offensive to a reasonable person.

118. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Defendant as part of its use of Defendant's services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

119. The Data Breach at the hands of Defendant constitutes an intentional interference

with Plaintiffs and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

120. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

121. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

122. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

123. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT III
Negligence Per Se
(On Behalf of Plaintiffs and the Nationwide Class)

124. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 87.

125. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

126. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Class Members due to the valuable nature of the PII at issue in this case.

127. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

128. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

129. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class Members.

130. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, financial crimes, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from financial

crimes and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

131. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

132. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 87.

133. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their PII with adequate data security.

134. Defendant knew that Plaintiffs and Class Members conferred a benefit on Defendant and accepted and have accepted or retained that benefit. Defendant profited from the purchases and used the PII of Plaintiffs and Class Members for business purposes.

135. The amounts Plaintiffs and Class Members paid for Defendant's goods and services should have been used, in part, to pay for the administrative costs of data management and security, including the proper and safe disposal of Plaintiffs' and Class Members' PII.

136. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement the data management and security measures that are mandated by industry standards.

137. Defendant failed to secure the PII of Plaintiffs and Class Members and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

138. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

139. If Plaintiffs and Class Members knew that Defendant would not secure their PII using adequate security, they would not have made purchases or developed a financial relationship with Defendant.

140. Plaintiffs and Class Members have no adequate remedy at law.

141. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, financial crimes, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate

the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from financial crimes and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

142. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

143. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from Plaintiffs and Class Members. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's goods and services.

COUNT V
Violations of New York Consumer Law for Deceptive Acts and Practices
New York Gen. Bus. Law § 349
(On Behalf of Plaintiffs and the Nationwide Class)

144. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 87.

145. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

146. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

147. Defendant stored Plaintiffs' and the Class members' PII in Defendant's electronic and consumer information databases. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and the Class members' PII secure and prevented the loss or misuse of Plaintiffs' and the Class members' PII. Defendant did not disclose to Plaintiffs and the Class members that its data systems were not secure.

148. Plaintiffs and the Class never would have provided their sensitive and personal PII if they had been told or knew that Defendant failed to maintain sufficient security to keep such PII from being hacked and taken by others, and that Defendant failed to maintain the information in encrypted form.

149. Defendant violated the NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendant's many systems and services, specifically the security thereof, and its ability to safely store Plaintiffs' and the Class members' PII.

150. Defendant also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiffs and the Class members of the Data Breach. If Defendant had

complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the damages related to the Data Breach.

151. Defendant's practices, acts, policies and course of conduct violate NYGBL § 349 in that:

a. Defendant actively and knowingly misrepresented or omitted disclosure of material information to Plaintiffs and the Class at the time they provided such PII that Defendant did not have sufficient security or mechanisms to protect PII;

b. Defendant failed to give timely warnings and notices regarding the defects and problems with its security systems that it maintained to protect Plaintiffs' and the Class Members' PII. Defendant possessed prior knowledge of the inherent defects in its IT systems and failed to address the same or to give timely warnings that the Data Breach occurred.

152. Plaintiffs and the Class Members were entitled to assume, and did assume, Defendant would take appropriate measures to keep their PII safe. Defendant did not disclose at any time that Plaintiffs' and the Class' PII was vulnerable to hackers because Defendant's data security measures were inadequate, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

153. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Defendant has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system it maintained and failed to reveal the Data Breach timely and adequately.

154. Members of the public were deceived by and relied upon Defendant's affirmative misrepresentations and failures to disclose.

155. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her PII to Defendant. Said deceptive acts and practices are material. The requests for and use of such PII in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

156. Defendant's wrongful conduct caused Plaintiffs and the Class to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the PII by third parties and placing the Plaintiffs and the Class at serious risk for monetary damages.

157. As a direct and proximate result of Defendant's violations of the above, Plaintiffs and Class members suffered damages including, but not limited to:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. money paid for goods purchased at Defendant's stores during the period of the Data Breach in that Plaintiffs and Class members would not have shopped at

Defendant's websites, or at least would not have used their payment cards for purchases, had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' PII and had Defendant provided timely and accurate notice of the Data Breach;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Security Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. damages to and diminution in value of their PII entrusted to Defendant for the sole purpose of purchasing products from Defendant's websites; and

i. the loss of Plaintiffs' and Class members' privacy.

158. In addition to or in lieu of actual damages, because of the injury, Plaintiffs and the Class seek statutory damages for each injury and violation which has occurred**.**

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against the Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiffs and Class members;

C. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to PII collection, storage, protection, and disposal, and to disclose with specificity to Plaintiffs and Class Members the type of PII compromised;

D. For an award of damages, including compensatory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: September 11, 2020

Respectfully Submitted,

/s/ *Amanda Peterson*

AMANDA PETERSON (AP1797)
MORGAN & MORGAN
90 Broad Street, Suite 1011
New York, NY 10004
(212) 564-4568
apeterson@ForThePeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
JEAN MARTIN
(*Pro Hac Vice application forthcoming*)
RYAN J. MCGEE
(*Pro Hac Vice application forthcoming*)

MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
jeanmartin@ForThePeople.com
rmcgee@ForThePeople.com

M. ANDERSON BERRY
(*Pro Hac Vice application forthcoming*))
LESLIE GUILLON
(*Pro Hac Vice application forthcoming*))
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
(916) 777-7777
aberry@justice4you.com
lguillon@justice4you.com